

# Power maps and subvarieties of the complex algebraic $n$ -torus

Iskander Aliev and Chris Smyth

April 27, 2008

## Summary

Given a subvariety  $V$  of the complex algebraic torus  $\mathbb{G}_m^n$  defined by polynomials of total degree at most  $d$  and a power map  $\phi : \mathbb{G}_m^n \rightarrow \mathbb{G}_m^n$ , the points  $\mathbf{x}$  whose forward orbits  $\mathcal{O}_\phi(\mathbf{x})$  belong to  $V$  form its *stable* subvariety  $S(V, \phi)$ . The main result of the paper provides an upper bound  $T = T(n, d, \phi)$  for the number of iterations of the power map  $\phi$  required to “cut off” the points of  $V$  that do not belong to  $S$ .

**2000 MS Classification:** Primary 11G35; Secondary 14L40.

## 1 Introduction

Given a set  $M$  and a map  $\phi : M \rightarrow M$ , one of the goals of dynamics is to classify the points  $\mathbf{x}$  of  $M$  according to the behavior of their forward orbits  $\mathcal{O}_\phi(\mathbf{x})$ . Let  $\mathbb{G}_m^n$  be the complex algebraic  $n$ -torus and  $z$  be an integer  $\geq 2$ . This paper is concerned with a special case of the general classification problem for  $M = \mathbb{G}_m^n$  and the  $z$ -th power map  $\phi : \mathbb{G}_m^n \rightarrow \mathbb{G}_m^n$  defined by the rule

$$\phi : (x_1, \dots, x_n) \longmapsto (x_1^z, \dots, x_n^z).$$

We refer the reader to Silverman [11] and Zhang [12] for results and further references on polynomial maps in algebraic dynamics.

As an affine variety, we will identify the torus  $\mathbb{G}_m^n$  with the Zariski open subset  $x_1 x_2 \cdots x_n \neq 0$  of affine space  $\mathbb{A}^n$ , with the usual multiplication

$$(x_1, x_2, \dots, x_n) \cdot (y_1, y_2, \dots, y_n) = (x_1 y_1, x_2 y_2, \dots, x_n y_n).$$

By *algebraic subvariety*, or simply *subvariety* of  $\mathbb{G}_m^n$ , we will understand a Zariski closed subset. An *algebraic subgroup* of  $\mathbb{G}_m^n$  is a Zariski closed subgroup. A *subtorus* of  $\mathbb{G}_m^n$  is a geometrically irreducible algebraic subgroup. Recall that the torsion points of  $\mathbb{G}_m^n$  are precisely the points  $\boldsymbol{\omega} = (\omega_1, \dots, \omega_n)$  whose coordinates

$\omega_i$  are roots of unity. By *torsion coset* we will mean a coset  $\omega H$ , where  $H$  is a subtorus of  $\mathbb{G}_m^n$  and  $\omega$  is a torsion point.

Both for convenience and for technical reasons we will often use Laurent polynomials through this paper. For a Laurent polynomial

$$f(\mathbf{X}) = \sum_{\mathbf{i}=(i_1,\dots,i_n) \in \mathbb{Z}^n} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}, \quad \mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n},$$

we will write

$$f^t = f(\phi^t(\mathbf{X})) = f(X_1^{z^t}, \dots, X_n^{z^t}).$$

The notation  $f \sim g$  for nonzero Laurent polynomials  $f$  and  $g$  will mean that  $f/g$  is either a constant or a monomial. A Laurent polynomial  $f$  will be called *nontrivial* if  $f \approx 1$ . The same notation will be applied to standard polynomials.

Now let  $f_1, f_2, \dots, f_s \in \mathbb{C}[X_1, \dots, X_n]$  be polynomials of total degree  $\leq d$ . For the subvariety  $V = Z(f_1, f_2, \dots, f_s) \subset \mathbb{G}_m^n$  and an integer  $u \geq 0$  we define the set

$$V(z, u) = \{\mathbf{x} \in \mathbb{G}_m^n : \phi^t(\mathbf{x}) \in V \text{ for } t = 0, \dots, u\}.$$

Clearly,  $V(z, u)$  is the subvariety of  $\mathbb{G}_m^n$  defined by the polynomials  $f_i^t$  for  $i = 1, \dots, s$  and  $t = 0, \dots, u$ . A subvariety  $S \subset V$  will be called  $(z, V)$ -stable if for all positive integers  $u$  we have  $S \subset V(z, u)$ . In other words, for any point  $\mathbf{x}$  of the subvariety  $S$  its forward orbit  $\mathcal{O}_\phi(\mathbf{x})$  belongs to  $V$ . We will call a  $(z, V)$ -stable subvariety  $S$  *maximal* if there is no  $(z, V)$ -stable subvariety  $S'$  with  $S \subsetneq S'$ . The maximal  $(z, V)$ -stable subvariety will be denoted by  $S(z, V)$ .

If for some integer  $T$  the subvariety  $S = V(z, T)$  is  $(z, V)$ -stable then clearly  $S = S(z, V)$ . The main result of the paper states that such an integer  $T$  can be effectively bounded in terms of the power  $z$ , the dimension  $n$  and the maximum total degree  $d$  of the defining polynomials  $f_1, f_2, \dots, f_s$  of the subvariety  $V$ .

**Theorem 1.1.** *There are effectively computable constants  $T = T(z, n, d)$ ,  $E = E(z, n, d)$  and  $L = L(z, n, d)$  such that*

- (i) *for any subvariety  $V$  of  $\mathbb{G}_m^n$  defined by the polynomials of total degree at most  $d$  we have  $S(z, V) = V(z, T)$ ;*
- (ii) *the subvariety  $S(z, V)$  is contained in a finite union of  $(n-1)$ -dimensional torsion cosets  $\bigcup_i D_i$ , where*

$$D_i = Z(h), \quad h \sim \mathbf{X}^{\mathbf{a}_i} - \zeta_i$$

*with  $\|\mathbf{a}_i\|_2 \leq L$ ,  $\zeta_i$  a  $z^k(z^l - 1)$ th root of unity, and  $k, l \leq E$ .*

For the sake of completeness in Section 3 we will give recurrent formulae for all the constants involved in the main theorem.

We will now discuss a relation between Theorem 1.1 and the classical theorem of Skolem–Mahler–Lech. Let us consider the sequence  $\{u_m\}$  defined as

$$u_m = a_1\alpha_1^m + \cdots + a_N\alpha_N^m \quad (m \in \mathbb{Z})$$

with nonzero coefficients  $a_i \in \mathbb{C}$  and with nonzero distinct elements  $\alpha_i \in \mathbb{C}$ . The sequence  $\{u_m\}$  is called *nondegenerate* if no quotient  $\alpha_i/\alpha_j$  ( $1 \leq i < j \leq N$ ) is a root of unity. Let  $S(u_m)$  denote the set of zeros of  $\{u_m\}$ , i.e., the set of solutions  $k \in \mathbb{Z}$  of the equation  $u_k = 0$ . The Skolem–Mahler–Lech theorem implies that for nondegenerate sequences  $\{u_m\}$  the set  $S(u_m)$  is finite. Furthermore, Theorem 1.2 of Evertse, Schlickewei and Schmidt [5] gives an upper bound for the cardinality of  $S(u_m)$  in terms of  $N$  only.

Let  $f(\mathbf{X}) = \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$  be a polynomial of total degree  $d$  and  $H = Z(f) \subset \mathbb{G}_{\mathbf{m}}^n$  be the hypersurface defined by  $f$ . Every point  $\beta$  of the stable subvariety  $S(z, H)$  clearly corresponds to a sequence  $\{u_m\}$  with infinite set  $S(u_m)$ . Moreover, the number of terms  $N$  of the sequence  $\{u_m\}$  will depend on  $n$  and  $d$  only. Consequently, the above mentioned theorem of Evertse, Schlickewei and Schmidt [5] gives us a restriction on the points that can lie on  $S(z, H)$ . Indeed, it implies that the ratio of at least two of the numbers  $\beta^{\mathbf{i}}$  ( $\mathbf{i}$  are integer vectors such that  $a_{\mathbf{i}} \neq 0$ ) must be a root of unity. Moreover, the upper bound for the cardinality of  $S(u_m)$  gives an upper bound for the number of iterations required to cut off the points that do not satisfy this restriction.

The next theorem shows that for  $n \leq 2$  the maximal stable subvarieties have remarkably simple structure.

**Theorem 1.2.** *Let  $V$  be a subvariety of  $\mathbb{G}_{\mathbf{m}}^n$ ,  $n \leq 2$ , and  $z$  be an integer  $\geq 2$ . Then the maximal  $(z, V)$ -stable subvariety  $S(z, V)$  is a finite union of torsion cosets.*

The general problem of finding all torsion cosets on a given subvariety of  $\mathbb{G}_{\mathbf{m}}^n$  has been addressed in Aliev and Smyth [1], Ruppert [8] and Sarnak and Adams [9]. For the special case  $n = 2$  the best among known algorithms is due to Beukers and Smyth [2]. Combining Theorem 1.2 and the algorithm of Beukers and Smyth we can find maximal stable subvarieties for the plane curves. For instance, let us consider the following example.

**Example:** Let  $f(X, Y) = X^2Y^2 + X^2Y + XY^2 + XY + X + Y + 1$ . The curve  $V = Z(f)$  has the largest known ratio

$$\frac{N_{\text{tor}}(f)}{\text{vol}(f)} = 16,$$

where  $N_{\text{tor}}(f)$  denote the number of torsion points on the curve  $Z(f)$  and  $\text{vol}(f)$  is the volume of the Newton polygon of the polynomial  $f$  (see Beukers and Smyth [2] for details). Indeed  $Z(f)$  contains exactly 48 torsion points of  $\mathbb{G}_{\mathbf{m}}^2$  listed below:

$$\begin{aligned}
& (\omega_{12}^{4i}, \omega_{12}^i), (\omega_{12}^i, \omega_{12}^{4i}), (-\omega_{12}^i, \omega_{12}^i), \quad i = 1, 5, 7, 11; \\
& (\omega_7^i, \omega_7^{2i}), (\omega_7^{2i}, \omega_7^i), \quad i = 1, \dots, 6; \\
& (-\omega_{30}^{3i}, \omega_{30}^i), (\omega_{30}^i, -\omega_{30}^{3i}), (\omega_{30}^i, \omega_{30}^{11i}), \quad i = 1, 7, 11, 13, 17, 19, 23, 29.
\end{aligned}$$

The power representation of torsion points lying on  $V$  allows us to easily detect the maximal  $(z, V)$ -stable subvarieties. For instance, it is clear that  $S(2, V)$  consists of 12 torsion points  $(\omega_7^i, \omega_7^{2i}), (\omega_7^{2i}, \omega_7^i), \quad i = 1, \dots, 6$ .

## 2 Lattices, algebraic subgroups of $\mathbb{G}_m^n$ and geometry of numbers

We recall some basic definitions. A *lattice* is a discrete subgroup of  $\mathbb{R}^n$ . Given a lattice  $L$  of rank  $r$ , any set of vectors  $\{\mathbf{b}_1, \dots, \mathbf{b}_r\}$  with  $L = \text{span}_{\mathbb{Z}}\{\mathbf{b}_1, \dots, \mathbf{b}_r\}$  or the matrix  $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_r)$  with rows  $\mathbf{b}_i$  will be called a *basis* of  $L$ . The *determinant* of a lattice  $L$  with a basis  $\mathbf{B}$  is defined to be

$$\det(L) = \sqrt{\det(\mathbf{B} \mathbf{B}^T)}.$$

When  $L$  is a lattice of rank  $n$ , its *polar* lattice  $L^*$  is defined as

$$L^* = \{\mathbf{x} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{y} \in L\},$$

where  $\langle \cdot, \cdot \rangle$  denotes the inner product. Given a basis  $\mathcal{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$  of  $L$ , the basis of  $L^*$  *polar* to  $\mathcal{B}$  is the basis  $\mathcal{B}^* = (\mathbf{b}_1^*, \dots, \mathbf{b}_n^*)$  such that

$$\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle = \delta_{ij}, \quad i, j = 1, \dots, n,$$

with  $\delta_{ij}$  the Kronecker delta.

By an *integer* lattice we understand a lattice  $A \subset \mathbb{Z}^n$ . An integer lattice is called *primitive* if  $A = \text{span}_{\mathbb{R}}(A) \cap \mathbb{Z}^n$ . Here  $\text{span}_{\mathbb{R}}(A)$  denotes the subspace of  $\mathbb{R}^n$  spanned by the vectors of the lattice  $A$ . For an integer lattice  $A$ , we define the subgroup  $H_A$  of  $\mathbb{G}_m^n$  by

$$H_A = \{\mathbf{x} \in \mathbb{G}_m^n : \mathbf{x}^{\mathbf{a}} = 1 \text{ for all } \mathbf{a} \in A\}.$$

Then, for instance,  $H_{\mathbb{Z}^n}$  is the trivial subgroup.

**Lemma 2.1.** *The map  $A \mapsto H_A$  sets up a bijection between integer lattices and algebraic subgroups of  $\mathbb{G}_m^n$ . A subgroup  $H = H_A$  is irreducible if and only if the lattice  $A$  is primitive.*

*Proof.* See Lemmas 1, 2 of Schmidt [10]. □

Let now  $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n)$  be a basis of the lattice  $\mathbb{Z}^n$ . The map  $\psi : \mathbb{G}_m^n \rightarrow \mathbb{G}_m^n$  defined by

$$\psi(\mathbf{x}) = (\mathbf{x}^{\mathbf{b}_1}, \dots, \mathbf{x}^{\mathbf{b}_n}) \quad (1)$$

is an automorphism of  $\mathbb{G}_m^n$  (see Ch. 3 in Bombieri and Gubler [3] and Section 2 in Schmidt [10]). The automorphism (1) is traditionally called a *monoidal transformation*. To make the inductive argument used in the proof of Theorem 1.1 more transparent, we will associate with  $\mathbf{B}$  the new coordinates  $(Y_1, \dots, Y_n)$  in  $\mathbb{G}_m^n$  defined by

$$Y_1 = \mathbf{X}^{\mathbf{b}_1}, \quad Y_2 = \mathbf{X}^{\mathbf{b}_2}, \dots, \quad Y_n = \mathbf{X}^{\mathbf{b}_n}. \quad (2)$$

Thus changing variables  $\mathbf{X} \mapsto \mathbf{Y}$  is equivalent to applying the automorphism  $\psi$  defined by (1).

Suppose that the matrix  $\mathbf{B}^{-1}$  has rows  $\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_n$ . By the *image* of a Laurent polynomial  $f \in \mathbb{C}[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$  in coordinates  $(Y_1, \dots, Y_n)$  we mean the Laurent polynomial

$$f^{\mathbf{B}}(\mathbf{Y}) = f(\mathbf{Y}^{\mathbf{r}_1}, \dots, \mathbf{Y}^{\mathbf{r}_n}).$$

and by the *image* of a subvariety  $V = Z(f_1, \dots, f_s)$  we understand the subvariety  $V^{\mathbf{B}}$  defined as the set of common zeroes in  $\mathbb{G}_m^n$  of the Laurent polynomials  $f_1^{\mathbf{B}}, \dots, f_s^{\mathbf{B}}$ . Then the subvariety  $V^{\mathbf{B}}$  is well defined and we will simply write  $V^{\mathbf{B}} = Z(f_1^{\mathbf{B}}, \dots, f_s^{\mathbf{B}})$ .

Let  $C = \omega H_A$  be an  $(n - r)$ -dimensional torsion coset and let  $(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_r)$  be a basis of the lattice  $A$ . Then  $C$  can be defined by  $r$  equations

$$\mathbf{X}^{\mathbf{a}_i} - \omega^{\mathbf{a}_i} = 0, \quad i = 1, \dots, r.$$

Each such an equation defines an  $(n - 1)$ -dimensional torsion coset in  $\mathbb{G}_m^n$  and, after a suitable automorphism, will have the form  $X_i = \omega_i$  with  $\omega_i$  a root of unity. This observation allows us to reduce the dimension of the problem provided that the subvarieties of interest lie in a torsion coset.

Let  $G^\perp$  denote the orthogonal complement of the subspace  $G \subset \mathbb{R}^n$ . We will need the following technical lemma from geometry of numbers.

**Lemma 2.2.** *Let  $G$  be a subspace of  $\mathbb{R}^n$  with  $\dim(G) = \text{rank}(G \cap \mathbb{Z}^n) = r < n$ . Then there exists a basis  $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$  of the lattice  $\mathbb{Z}^n$  such that  $\mathbf{a}_1 \in G^\perp$  and the vectors of the polar basis  $\mathbf{A}^* = (\mathbf{a}_1^*, \mathbf{a}_2^*, \dots, \mathbf{a}_n^*)$  satisfy the inequalities*

$$\|\mathbf{a}_i^*\|_2 < 1 + \frac{n-1}{2} \gamma_{n-1}^{\frac{n-1}{2}} \gamma_{n-r}^{\frac{1}{2}} \det(G \cap \mathbb{Z}^n)^{\frac{1}{n-r}}, \quad i = 1, \dots, n. \quad (3)$$

with  $\gamma_{n-1}$  the Hermite constant for dimension  $n - 1$  (for the definition and properties of the Hermite constant see Section 38.1 of Gruber–Lekkerkerker [7]).

*Proof.* See Corollary 2.1 of Aliev and Smyth [1].  $\square$

### 3 Proof of Theorem 1.1

In this section we will show that the statement of Theorem 1.1 holds for the constants  $T$ ,  $E$  and  $L$  defined as follows. We can take  $T(z, 1, d) = d$  and

$$T(z, n, d) = c_0(z, d)T(z^{c_0(z, d)}, n-1, c_1(z, n, d)z^{2c_0(z, d)-1}) \\ + c_0(z, d),$$

where  $c_0(z, d) = \lceil 3 \log(d) / \log(z) \rceil + d(d-1)$  and  $c_1(z, n, d) = n(n+1)d + \lceil n(n^2 - 1)\gamma_{n-1}^{\frac{n-1}{2}} dL(z, n, d) \rceil$ . The constants  $E$  and  $L$  can be calculated as

$$E(z, n, d) = E(z, n-1, d^5 z^{d(d-1)}), \quad E(z, 1, d) = d;$$

$$L(z, n, d) = L(z, n-1, d^5 z^{d(d-1)}), \quad n \geq 3,$$

$$L(z, 2, d) = 2d, \quad L(z, 1, d) = 1.$$

It is clearly enough to prove the theorem in the case when  $V$  is a hypersurface in  $\mathbb{G}_m^n$ . We will start with the following auxiliary result which slightly extends the Proposition 1 of Ruppert [8].

**Lemma 3.1.** *Let  $f \in \mathbb{C}[X_1, X_2, \dots, X_n]$ ,  $n \geq 2$ , be a nontrivial irreducible polynomial and  $\eta_1, \dots, \eta_n$  be the  $M$ th roots of unity. If  $f$  divides the polynomial  $f(\eta_1 X_1^N, \eta_2 X_2^N, \dots, \eta_n X_n^N)$  for some integer  $N > 1$  then  $f$  has the form*

$$f \sim \mathbf{X}^{\mathbf{a}} - \zeta,$$

where  $\mathbf{a}$  is an integer vector and  $\zeta$  is a root of unity with  $\zeta^{(N-1)M} = 1$ .

*Proof.* We will modify the proof of the Proposition 1 of Ruppert [8]. It consists of seven steps and only the first and the last of them need to be changed.

The first step allows us to assume that the polynomial  $f$  cannot be represented in the form  $f = g(X_1^{a_1}, \dots, X_n^{a_n})$  with some  $a_i > 1$ . To see this observe that in our case the polynomial  $g$  will divide the polynomial  $g(\eta_1^{a_1} X_1^N, \eta_2^{a_2} X_2^N, \dots, \eta_n^{a_n} X_n^N)$  and  $\eta_1^{a_1}, \eta_2^{a_2}, \dots, \eta_n^{a_n}$  are the  $M'$ th roots of unity with  $M' | M$ . Therefore we can simply replace  $f$  by  $g$ .

The next five steps of the original proof will remain almost unchanged - we just always replace the polynomial  $f(X_1^N, X_2^N, \dots, X_n^N)$  by the polynomial  $f(\eta_1 X_1^N, \eta_2 X_2^N, \dots, \eta_n X_n^N)$ .

At the seventh step we may assume that  $f = X_1 \cdots X_m - dX_{m+1} \cdots X_n$  and, consequently,  $f(\eta_1 X_1^N, \eta_2 X_2^N, \dots, \eta_n X_n^N) = \mu_1(X_1 \cdots X_m)^N - d\mu_2(X_{m+1} \cdots X_n)^N$ , where  $\mu_i$  are the  $M$ th roots of unity. After the substitution  $X_2 = \mu_1^{-1/N}$ ,  $X_3 = 1, \dots, X_{n-1} = 1$ ,  $X_n = \mu_2^{-1/N}$ , we have  $\mu_1^{-1/N} X_1 - d\mu_2^{-1/N} | X_1^N - d$ . Therefore,  $d^{(N-1)M} = \mu_2^M = 1$ .

□

The next lemma show that, roughly speaking, for all sufficiently large  $t$  the irreducible common factors of the polynomials  $f, f^1, f^2, \dots, f^t$  will define the  $(n - 1)$ -dimensional torsion cosets.

**Lemma 3.2.** *Let  $f \in \mathbb{C}[X_1, \dots, X_n]$ ,  $n \geq 2$ , be a (possibly reducible) polynomial of the total degree  $d$ . Then*

- (i) *for any integer  $t \geq t_0 = \lceil 3 \log(d) / \log(z) \rceil$  each irreducible common factor of the polynomials  $f$  and  $f^t$  consists of precisely two terms;*
- (ii) *there exists an integer,  $t$ , with  $t_0 \leq t_1 \leq c_0 = c_0(z, d)$  such that each irreducible common factor  $g$  of the polynomials  $f$  and  $f^{t_1}$  has the form*

$$g \sim \mathbf{X}^{\mathbf{a}} - \zeta, \quad (4)$$

where  $\mathbf{a}$  is an integer vector and  $\zeta$  is a  $z^k(z^l - 1)$ th root of unity with  $0 \leq k, l \leq c_0$ .

*Proof.* (i) Suppose that the statement is wrong. Then for some irreducible factors  $g_1$  and  $g_2$  of the polynomial  $f$  we would have  $g_1 | g_2^t$  with  $t \geq t_0$  and  $g_1$  consisting of more than two terms. Furthermore, by the first result stated in Section III of Gourin [6], the polynomial  $g_2$  must consist of more than two terms as well.

Observe that  $\deg(g_2^t) \geq z^{t_0} \geq d^3$  and thus  $g_1 \neq g_2^t$ , so that the polynomial  $g_2^t$  is reducible. By Theorem I of Gourin [6] there exist nonnegative integers  $t_1, t_2, \dots, t_n$  such that

$$z^{t_i} \leq d^2, \quad i = 1, \dots, n \quad (5)$$

and  $g_1$  can be obtained by replacing each  $X_i$  by  $X_i^{z^{t-t_i}}$  in an irreducible factor  $g_2^*$  of the polynomial  $g_2(X_1^{z^{t_1}}, \dots, X_n^{z^{t_n}})$ . Therefore we must have  $\deg(g_1) > z^{t-t_i}$ . However by (5)

$$z^{t-t_i} \geq \frac{z^{t_0}}{d^2} \geq d.$$

The contradiction obtained proves part (i).

(ii) The polynomial  $f$  can be written in the form

$$f = h_1 h_2 \cdots h_k f',$$

where each of the polynomials  $h_i$  consists of precisely two terms and each of factors of the polynomial  $f'$  have more than two terms. Let us choose an integer  $s_0$  with  $t_0 \leq s_0 \leq c_0$ . By part (i) and the first result stated in Section III of Gourin [6], for some  $1 \leq i, j \leq k$  we have  $h_i | h_j^{s_0}$ . Put  $g = h_i$  and suppose first that  $i = j$  so that  $g | g^{s_0}$ . Then by Proposition 1 of Ruppert [8] the polynomial  $g$  has the form (4) with  $\zeta^{z^{s_0}-1} = 1$ . Thus we can take  $t_1 = l = s_0$  and  $k = 0$ . To settle the case  $i \neq j$  suppose that  $g | h_j^{s_1}$  for some integer  $s_1 > s_0$ . We will show

that this implies that the polynomial  $g$  has the desired form. By Lemma I of Gourin [6] we have

$$h_j^{s_1} = \prod_v g_v^{s_1 - s_0},$$

where the polynomials  $g_v$  are irreducible and form the *complete set of*  $z^{s_0} \dots z^{s_0}$  *transforms*, as introduced in Gourin [6] p. 486, obtained from the polynomial  $g$ . Therefore  $g$  divides a polynomial  $g(\eta_1 X_1^{z^{s_1-s_0}}, \eta_2 X_2^{z^{s_1-s_0}}, \dots, \eta_n X_n^{z^{s_1-s_0}})$  where  $\eta_i$  are  $z^{s_0}$ th roots of unity. Now by Lemma 3.1 the polynomial  $g$  must have the form

$$g \sim \mathbf{X}^{\mathbf{a}} - \zeta,$$

where  $\mathbf{a}$  is an integer vector and  $\zeta$  is a root of unity with  $\zeta^{z^{s_0}(z^{s_1-s_0}-1)} = 1$ .

The number  $k$  of the factors  $h_i$  does not exceed  $d$ . Therefore, among the integers  $t_0, t_0+1, \dots, t_0+d(d-1) = c_0$  there always exists an integer  $t_1$  satisfying the conditions of the lemma. Finally we take  $k = s_0$  and  $l = s_1 - s_0$ .  $\square$

Let now  $f \in \mathbb{C}[X_1, \dots, X_n]$  be a polynomial of total degree  $d$  and  $V = Z(f)$ . We will proceed by induction on the number of variables  $n$ .

At the basis step  $n = 1$  the defining polynomial  $f = f(X)$  has degree  $d$  and  $T(z, 1, d) = d$  as well. Therefore, a root  $\omega$  of  $f$  belongs to  $S = V(z, T(z, 1, d))$  if and only if for some integers  $k \geq 0, l > 0$  with  $k + l \leq d$  we have  $\omega^{z^{k+l}} = \omega^{z^k}$ . Therefore  $S$  is  $(z, V)$ -stable and consists of  $z^k(z^l - 1)$ th roots of unity with  $k, l \leq d = E(z, 1, d)$ . Each such a root  $\omega$  can be regarded as a 0-dimensional torsion coset  $Z(X - \omega)$  in  $\mathbb{G}_m$ . Thus  $L(z, 1, d) = 1$ .

Suppose now that  $n \geq 2$ . At the inductive step we will first decompose the problem into two cases. Let us consider the polynomial  $g = \gcd(f, f^{t_1})$ , where  $t_1$  is the integer satisfying conditions of the part (ii) of Lemma 3.2. The polynomial  $g$  can be written as  $g = h_1 h_2 \dots$ , where each of the factors  $h_i$  is irreducible and has the form (4). Observe that any irreducible component  $U$  of the subvariety  $S = V(z, T(z, n, d))$  belongs to at least one of the subvarieties  $Z(g)$  and  $Z(f/g, f^{t_1}/g)$ . Thus we can separately consider the case  $U \subset Z(g)$  and the case  $U \subset Z(f/g, f^{t_1}/g) \setminus Z(g)$ .

Suppose that  $U \subset Z(g)$ . Since  $U$  is irreducible, there is a factor  $h_i$  of  $g$  with  $U \subset Z(h_i)$  and

$$h_i \sim h = \mathbf{X}^{\mathbf{a}} - \zeta.$$

Here  $\zeta$  is a  $z^k(z^l - 1)$ th root of unity with  $0 \leq k, l \leq t_0 + d(d-1)$ , so that  $k, l \leq E(z, n, d)$ . Observe that  $\|\mathbf{a}\|_1 \leq 2 \deg(h_i) \leq 2d$  and thus

$$\|\mathbf{a}\|_2 \leq 2d \leq L(z, n, d). \quad (6)$$

Thus the component  $U$  lies in the torsion coset  $Z(h)$  satisfying the conditions of Theorem 1.1. Let us show that  $U$  is  $(z, V)$ -stable.



By Lemma 2.2 applied to the subspace  $G = (\text{span}_{\mathbb{R}}(\mathbf{a}))^\perp$ , there exists a basis  $\mathbf{A} = (\mathbf{a}_1, \dots, \mathbf{a}_{n-1})$  of the lattice  $\mathbb{Z}^n$  such that  $\mathbf{a}_1 = \mathbf{a}$  and its polar basis  $\mathbf{A}^* = (\mathbf{a}_1^*, \dots, \mathbf{a}_n^*)$  satisfies the inequality (2.2).

Let  $(Y_1, \dots, Y_n)$  be the coordinates associated with  $\mathbf{A}$ . Clearly, the subvariety  $S$  is  $(z, V)$ -stable if and only if  $S^{\mathbf{A}}$  is  $(z, V^{\mathbf{A}})$ -stable.

Consider the subvariety  $X = S^{\mathbf{A}} \cap Z(Y_1 - \zeta)$ . The preimage of  $X$  in the initial coordinates is the subvariety  $S \cap Z(h)$ . Thus  $U^{\mathbf{A}}$  is an irreducible component of  $X$  and it is enough to show that  $X$  is  $(z, V^{\mathbf{A}})$ -stable.

Recall that  $\zeta$  is a  $z^k(z^l - 1)$ th root of unity. Therefore we can write  $X = P \cap C$ , where

$$P = \{(\zeta, Y_2, \dots, Y_n) \in \mathbb{G}_{\mathbf{m}}^n : f^{\mathbf{A}}(\zeta^{z^u}, Y_2^{z^u}, \dots, Y_n^{z^u}) = 0, u = 0, \dots, k-1\}$$

and

$$C = \{(\zeta, Y_2, \dots, Y_n) \in \mathbb{G}_{\mathbf{m}}^n : f^{\mathbf{A}}(\zeta^{z^{k+v}}, Y_2^{z^{k+v}}, \dots, Y_n^{z^{k+v}}) = 0, \\ v = 0, \dots, T(z, n, d) - k\}.$$

Now it is clearly enough to show that  $C$  is  $(z, V^{\mathbf{A}})$ -stable.

Observe that  $\nu = \zeta^{z^k}$  is a  $(z^l - 1)$ th root of unity and  $\gcd(z^l - 1, z) = 1$ . Therefore, denoting  $W_i = Z(f^{\mathbf{A}}(\nu^{z^i}, Y_2^{z^{k+i}}, \dots, Y_n^{z^{k+i}})) \subset \mathbb{G}_{\mathbf{m}}^{n-1}$ , we will have

$$C = \left\{ (\zeta, Y_2, \dots, Y_n) \in \mathbb{G}_{\mathbf{m}}^n : (Y_2, \dots, Y_n) \in \bigcap_{i=0}^{l-1} W_i(z^l, T_i^*) \right\}$$

with  $T_i^* \geq \lfloor (T(z, n, d) - k)/l \rfloor$ .

If for each  $i$  the subvariety  $S_i = W_i(z^l, T_i^*)$  is  $(z^l, W_i)$ -stable, then, clearly, the subvariety  $C$  is  $(z, V^{\mathbf{A}})$ -stable.

It is well known (see e. g. Bombieri and Vaaler [4], pp. 27–28) that  $\det(G \cap \mathbb{Z}^n) = \det(G^\perp \cap \mathbb{Z}^n)$ . Thus  $\det(G) = \|\mathbf{a}\|_2$  and (2.2) together with (6) implies

$$S_{f^{\mathbf{A}}} \subset (n \max_{1 \leq j \leq n-1} \|\mathbf{a}_j^*\|_\infty) dB_1^n \subsetneq (nd + n(n-1)\gamma_{n-1}^{\frac{n-1}{2}} d^2) B_1^n.$$

Here  $B_1^n$  denotes the unit  $n$ -ball with respect to the  $l_1$ -norm. Multiplying  $f^{\mathbf{A}}$  by a monomial, we may assume that  $f^{\mathbf{A}} \in \mathbb{C}[Y_1, \dots, Y_n]$  with

$$\deg(f^{\mathbf{A}}) < c_2(n, d) = n(n+1)d + \lfloor n(n^2 - 1)\gamma_{n-1}^{\frac{n-1}{2}} d^2 \rfloor.$$

Recall that  $k, l \leq t_0 + d(d-1)$  by part (ii) of Lemma 3.2. Thus  $lT(z^l, n-1, c_2(n, d)z^{k+l-1}) + k \leq T(z, n, d)$  and, consequently, we have  $T_i^* \geq T(z^l, n-1, c_2(n, d)z^{k+l-1})$ . Finally, by the inductive assumption, for each  $i$  the subvariety  $S_i$  is  $(z^l, W_i)$ -stable.

Suppose now that  $U \subset Z(f/g, f^{t_1}/g) \setminus Z(g)$ . Let  $r \in \mathbb{C}[X_1, \dots, X_{n-1}]$  be the resultant of the polynomials  $f/g$  and  $f^{t_1}/g$  with respect to the variable  $X_n$ . The polynomial  $r$  is not identically zero and has the total degree  $\deg(r) \leq d^2 z^{t_1}$ . The

orthogonal projection  $\pi(U)$  into the coordinate subspace corresponding to the indeterminates  $X_1, \dots, X_{n-1}$  clearly lies on the hypersurface  $R = Z(r)$  in  $\mathbb{G}_m^{n-1}$ . In order to apply the inductive assumption we observe first that  $T(z, n, d) \geq T(z, n-1, \deg(r)) + t_1$  and thus  $\pi(U) \subset Q = R(z, T(z, n-1, \deg(r)))$ .

By the inductive assumption  $Q$  is  $(z, R)$ -stable and lies in a finite union  $\bigcup D_i$  of  $(n-2)$ -dimensional torsion cosets in  $\mathbb{G}_m^{n-1}$  satisfying conditions of Theorem 1.1. Since  $U$  is irreducible, there should be a torsion coset  $D = D_j$  with  $\pi(U) \subset D$ . Suppose that  $D = Z(h)$  with  $h \sim (X_1, \dots, X_{n-1})^{\mathbf{a}} - \zeta$ . Then the component  $U$  lies in the  $n-1$  dimensional coset  $D'$  in  $\mathbb{G}_m^n$  defined by the same polynomial  $h$  regarded as a polynomial in  $\mathbb{C}[X_1, \dots, X_n]$ . Moreover the coset  $D'$  satisfies conditions of the part (ii) of Theorem 1.1. Let us show now that  $U$  is  $(z, V)$ -stable.

We have  $D = \omega H_B$ , where  $B$  is a primitive sublattice of  $\mathbb{Z}^{n-1}$  with  $B = \text{span}_{\mathbb{Z}}(\mathbf{a})$  and  $\det(B) = \|\mathbf{a}\|_2 \leq L(z, n-1, \deg(r))$ . By Lemma 2.2, applied to the subspace  $G = (\text{span}_{\mathbb{R}}(B))^{\perp}$ , there exists a basis  $\mathbf{A} = (\mathbf{a}_1, \dots, \mathbf{a}_{n-1})$  of the lattice  $\mathbb{Z}^{n-1}$  such that  $\mathbf{a}_1 = \mathbf{a}$  and its polar basis  $\mathbf{A}^* = (\mathbf{a}_1^*, \dots, \mathbf{a}_{n-1}^*)$  satisfies the inequality (2.2).

The basis  $\mathbf{A}$  of  $\mathbb{Z}^{n-1}$  can be extended to the basis

$$\mathbf{B} = ((\mathbf{a}_1, 0), \dots, (\mathbf{a}_{n-1}, 0), \mathbf{e}_n)$$

of  $\mathbb{Z}^n$ , where  $(\mathbf{a}_i, 0)$  denotes the vector  $(a_{i1}, \dots, a_{in-1}, 0)$  and  $\mathbf{e}_n = (0, \dots, 0, 1)$ .

Let  $(Y_1, \dots, Y_n)$  be the coordinates associated with  $\mathbf{B}$ . The rest of the proof follows the scheme used in the previous case with minor changes. However we will give the full proof here for completeness. As above, we consider the subvariety  $X = S^{\mathbf{B}} \cap Z(Y_1 - \zeta)$  and observe that the preimage of  $X$  in the initial coordinates is the subvariety  $S \cap Z(h)$ . This implies that  $U^{\mathbf{B}}$  is an irreducible component of  $X$  and thus it is enough to prove that  $X$  is  $(z, V^{\mathbf{B}})$ -stable.

By the inductive assumption  $\zeta$  is a  $z^k(z^l - 1)$ th root of unity. Therefore, similar to the previous case, we can write  $X = P \cap C$ , where

$$P = \{(\zeta, Y_2, \dots, Y_n) \in \mathbb{G}_m^n : f^{\mathbf{B}}(\zeta^{z^u}, Y_2^{z^u}, \dots, Y_n^{z^u}) = 0, u = 0, \dots, k-1\}$$

and

$$C = \{(\zeta, Y_2, \dots, Y_n) \in \mathbb{G}_m^n : f^{\mathbf{B}}(\zeta^{z^{k+v}}, Y_2^{z^{k+v}}, \dots, Y_n^{z^{k+v}}) = 0, \\ v = 0, \dots, T(z, n, d) - k\}.$$

The inductive assumption will allow us to show that  $C$  is  $(z, V^{\mathbf{B}})$ -stable. The stability of  $C$  then implies the stability of  $X$ .

Since  $\nu = \zeta^{z^k}$  is a  $(z^l - 1)$ th root of unity, it is convenient to introduce the subvarieties  $W_i = Z(f^{\mathbf{B}}(\nu^{z^i}, Y_2^{z^{k+i}}, \dots, Y_n^{z^{k+i}})) \subset \mathbb{G}_m^{n-1}$  and to represent  $C$  in the form

$$C = \left\{ (\zeta, Y_2, \dots, Y_n) \in \mathbb{G}_m^n : (Y_2, \dots, Y_n) \in \bigcap_{i=0}^{l-1} W_i(z^l, T_i^*) \right\},$$

where as above  $T_i^* \geq \lfloor (T(z, n, d) - k)/l \rfloor$ .

Further, the subvariety  $C$  is  $(z, V^{\mathbf{A}})$ -stable if each of the subvarieties  $S_i = W_i(z^l, T_i^*)$ ,  $0 \leq i \leq l-1$ , is  $(z^l, W_i)$ -stable. Thus we need a bound for the size of  $\text{supp}(f^{\mathbf{B}})$ .

We have  $\det(G) = \|\mathbf{a}\|_2$  and by (2.2)

$$S_{f^{\mathbf{B}}} \subset (n \max_{1 \leq j \leq n-1} \|\mathbf{a}_j^*\|_\infty) dB_1^n \subsetneq (nd + n(n-1)\gamma_{n-1}^{\frac{n-1}{2}} dL(z, n-1, \deg(r))) B_1^n.$$

Multiplying  $f^{\mathbf{B}}$  by a monomial, we may assume that  $f^{\mathbf{B}} \in \mathbb{C}[Y_1, \dots, Y_n]$  with

$$\deg(f^{\mathbf{B}}) < c_1(z, n, d).$$

Recall that  $k \leq t_0 + d(d-1)$  and  $l \leq d(d-1)$  by part (ii) of Lemma 3.2. Thus  $lT(z^l, n-1, c_1(z, n, d)z^{k+l-1}) + k \leq T(z, n, d)$  and, by the inductive assumption, for each  $i$  the subvariety  $S_i$  is  $(z^l, W_i)$ -stable.

## 4 Proof of Theorem 1.2

Since the intersection of torsion cosets is a torsion coset itself, we may assume that  $V$  is a hypersurface. The statement of the theorem is clearly true for  $n = 1$ . In this case the subvariety  $S(z, V)$ , if not empty, consists of a finite number of roots of unity.

Suppose now that  $n = 2$  and  $V = Z(f)$  with  $f \in \mathbb{C}[X_1, X_2]$ . Let  $S_1$  be an irreducible component of the subvariety  $S(z, V)$ . By the part (ii) of Theorem 1.1, the component  $S_1$  lies in an one-dimensional torsion coset  $D = Z(X_1^{a_1} X_2^{a_2} - \zeta)$  where  $\zeta$  is a root of unity,  $a_1, a_2 \in \mathbb{Z}$  and, by Lemma 2.1, we have  $\gcd(a_1, a_2) = 1$ . The integer vector  $\mathbf{a} = (a_1, a_2)$  can be extended to a basis  $\mathbf{B} = (\mathbf{a}, \mathbf{b})$  of the lattice  $\mathbb{Z}^2$ . If  $(Y_1, Y_2)$  are the coordinates associated with the basis  $\mathbf{B}$  then clearly  $S_1^{\mathbf{B}} \subset Z(Y_1 - \zeta)$ . If  $Z(Y_1 - \zeta) \subset S^{\mathbf{B}}$  then  $S_1^{\mathbf{B}} = Z(Y_1 - \zeta)$  and the theorem is proved. Thus we may assume without loss of generality that  $Z(Y_1 - \zeta) \not\subset S^{\mathbf{B}}$ .

Let  $g = f^{\mathbf{B}}$ . By the above assumption, for some  $u$  the polynomial  $Y_1 - \zeta$  does not divide the polynomial  $g^u$ . Next, by part (ii) of Lemma 3.2 for some  $v$  with  $v > u$  all irreducible common factors of the polynomials  $g^u$  and  $g^v$  define one-dimensional torsion cosets. Let  $h$  be such a factor and suppose that  $S_1 \subset Z(h)$ . Since  $h \sim Y_1^{b_1} Y_2^{b_2} - \mu$ , where  $\mu$  is a root of unity, we will have  $S_1 = (\zeta, \eta)$  for some root of unity  $\eta$ . Thus we only need to settle the case  $S_1 \not\subset Z(\gcd(g^u, g^v))$ . Let  $r \in \mathbb{C}[Y_2]$  be the resultant of the polynomials  $g^u / \gcd(g^u, g^v)$  and  $g^v / \gcd(g^u, g^v)$  with respect to the variable  $Y_1$ . The orthogonal projection of the component  $S_1$  into the coordinate axis  $Y_2$  clearly lies on the maximal  $(z, Z(r))$ -stable subvariety  $S(z, Z(r))$ . Since  $S(z, Z(r))$  is a finite union of roots of unity, the component  $S_1$  is a torsion point of  $\mathbb{G}_m^2$ .

## 5 Acknowledgement

The authors are very grateful to Professor Thomas Tucker for important comments.

## References

- [1] *I. Aliev, C. Smyth*, Torsion points on subvarieties of  $\mathbb{G}_m^n$ , submitted (arXiv:0704.1747v2 [math.NT]).
- [2] *F. Beukers, C. J. Smyth*, Cyclotomic points on curves, Number theory for the millennium, I (Urbana, IL, 2000), 67–85, A K Peters, Natick, MA, 2002.
- [3] *E. Bombieri, W. Gubler*, Heights in Diophantine geometry, New Mathematical Monographs, 4. Cambridge University Press, Cambridge, 2006.
- [4] *E. Bombieri, J. Vaaler*, On Siegel’s Lemma, Invent. Math. 73 (1983) 11–32, Addendum, ibid. 75 (1984) 377.
- [5] *J. H. Evertse, H. P. Schlickewei, W. M. Schmidt*, Linear equations in variables which lie in a multiplicative group, Ann. of Math. (2) **155** (2002), no. 3, 807–836.
- [6] *E. Gourin*, On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves, Trans. Amer. Math. Soc. **32** (1930), no. 3, 485–501.
- [7] *P. M. Gruber, C. G. Lekkerkerker*, Geometry of numbers, North-Holland, Amsterdam 1987.
- [8] *W. M. Ruppert*, Solving algebraic equations in roots of unity, J. Reine Angew. Math. **435** (1993), 119–156.
- [9] *P. Sarnak, S. Adams*, Betti numbers of congruence groups, with an appendix by Ze’ev Rudnick, Israel J. Math. **88** (1994), no. 1-3, 31–72.
- [10] *W. M. Schmidt*, Heights of points on subvarieties of  $\mathbb{G}_m^n$ , Number theory (Paris, 1993–1994), 157–187, London Math. Soc. Lecture Note Ser., 235, Cambridge Univ. Press, Cambridge, 1996.
- [11] *J. H. Silverman*, The arithmetic of dynamical systems, Graduate Texts in Mathematics, 241. Springer, New York, 2007.
- [12] *S. Zhang*, Distributions in Algebraic Dynamics, A tribute to Professor S. S. Chern, Survey in Differential Geometry, vol 10, 381–430, International Press 2006.

School of Mathematics and Wales Institute of Mathematical and Computational Sciences, Cardiff University, Senghennydd Road, Cardiff CF24 4AG UK

*E-mail address:* alievi@cf.ac.uk

School of Mathematics and Maxwell Institute for Mathematical Sciences, University of Edinburgh, Kings Buildings, Edinburgh EH9 3JZ UK

*E-mail address:* C.Smyth@ed.ac.uk